

**Appendix F to DIR Contract Number DIR-TSO-2736
ADVANCED RECOVERY SERVICES CONTENT (NORTH AMERICA)**

A. NETWORK SERVICES

| |
|---|
| Cross Connect Services – Features |
| <p>Sungard AS will provide the following for the number of cross connects identified in the Order, in accordance with the Customer completed design requirements form:</p> <ul style="list-style-type: none"> • Provision and install cross connects between telecommunication circuit(s) and Customer's environment located in the Designated Sungard AS Facility; and • Assistance with telecommunication circuit acceptance testing. |
| Dedicated Transport Services – Features |
| <p>Sungard AS will provide the following for the number of telecommunication circuits identified in the Order, in accordance with the Customer completed design requirements form:</p> <ul style="list-style-type: none"> • Installation of the telecommunications circuit(s) into the Designated Sungard AS Facility; • Coordinate telecommunication carrier acceptance testing; and • Provision and install cross connects between the telecommunication circuit(s) and Customer's environment, each located in the Designated Sungard AS Facility. |
| Metrobandwidth – Features |
| <p>Within 2 hours of a Customer request to make use of certain Services identified on this Order that Customer intends to connect to Customer's colocation or hot site environment hosted within the same Designated Sungard AS Facility or campus, Sungard AS will provide the type of network connectivity identified in the Order.</p> |
| Metrobandwidth – General |
| <p>One or more other customers ("other affected customers") may require use of the same network connectivity infrastructure ("Metrobandwidth Resources") at the same time as Customer. The following provisions are intended to avoid or minimize contention for Metrobandwidth Resources:</p> <ul style="list-style-type: none"> • All Metrobandwidth Resources are designated by Sungard AS as "Priority Resources" or "Shared Resources" and are subject to change without notice, provided that Sungard AS shall not change the designation of a Metrobandwidth Resource at any time that a Metrobandwidth Resources is being used by a customer; • Customer will have exclusive rights of access to and use of Metrobandwidth Resources designated by Sungard AS as Priority Resources that are not then being used by other affected customers; • Customer and all other customers requesting use will have equal rights of access to and use of Shared Resources, irrespective of the order in which use was requested, in such cases, Customer will reasonably cooperate with Sungard AS and the other affected customers in the use of the Shared Resources; and • Sungard AS will maintain records of its receipt of requests, which will be the exclusive basis for determining the order in which requests were received. |
| <p>Customer may use the Metrobandwidth Resources for so long as the Services on this Order and the Customer colocation or hot site environment hosted within the same Designated Sungard AS Facility or campus are available for use.</p> |
| Managed Internet Access Services – Features |
| <p>Sungard AS will provide the amount of bandwidth identified in the Order and, for Sungard AS-provided IP addresses, will provide the following, in accordance with the Customer completed design requirements form:</p> <ul style="list-style-type: none"> • 8 IP addresses unless otherwise identified in Part 1 of the Order; • Registered Autonomous System Number (ASN) (only applicable for customers who require BGP peering); |

- Monthly report of bandwidth utilization;
- Up to 5 DNS changes with up to 10 records per change per month, for Customer-registered domain names; and
- Domain name administration services for up to 10 primary and/or secondary Customer domain(s).

Basic Internet Service – Features

Sungard AS will provide the amount of bandwidth identified in Part 1 of the Order and, for Sungard AS-provided IP addresses, will provide the following, in accordance with the Customer completed design requirements form:

- Single network port connection to the Internet with 100/1000 port speeds;
- Sungard AS provided IP address in accordance with the Sungard AS IPv4 Address Space Request Policy; and
- SNMP/ICMP Monitoring.

Managed Internet Access Services & Basic Internet Services – General

If indicated in the Order, Customer may burst above the committed bandwidth tier up to the burstable limit identified in the Order, subject to available bandwidth on Sungard AS' network. An Incremental burstable usage fee will be invoiced in arrears for each Mbps exceeding the committed bandwidth tier. Customer's burstable usage is determined on a monthly basis by traffic samples taken every 5 minutes and ranking the traffic samples from highest to lowest and calculating the fee based on the usage that falls at the 95th highest percentile.

Sungard AS assigns IP addresses in accordance with the requirements of American Registry for Internet Numbers (ARIN) and Réseaux IP Européens or European IP Networks (RIPE), and, in the case of IPv4 IP addresses, in accordance with Sungard AS' IPv4 IP Address Space Request Policy. IPv4 address blocks containing more than 8 IP addresses are not guaranteed and are only available based on Sungard AS receipt of adequate Customer-provided justification. If Customer has significant IP requirements (for example, in excess of 256 public IP addresses), Sungard AS may require that Customer contact ARIN directly to register the IP addresses.

Network addresses assigned from Sungard AS are non-portable. Network space allocated to Customer by Sungard AS must be returned to Sungard AS in the event the Managed Internet Access or Basic Internet Services are terminated or cancelled.

Upon at least 60 days advance notice, Sungard AS reserves the right to re-groom the Service, at Sungard AS' sole expense, to an alternate network node provided that Sungard AS shall not arbitrarily or discriminatorily perform such changes and that Sungard AS shall work in good faith with Customer to minimize any disruption to the Services. Customer shall have the right to terminate the Basic or Managed Internet Service without penalty by providing notice within 30 days after receipt of Sungard AS' notice.

LAN Services and WAN Services – Features

Sungard AS will provide the following for the number of network termination devices identified in the Order in accordance with the Customer completed design requirements form:

- Maintain network equipment software configuration backup;
- Exclusive control of administrator security passwords and IDs (Customer may request a copy of device configuration data);
- Monitor critical patch alerts and provide Customer notification of such patches;
- If identified in the Order, provision of the network termination devices;
- Coordination of third party equipment vendor maintenance and detected equipment problem resolution;
- Hardware Installation Services (if the equipment is located in the Designated Sungard AS Facility);
- Equipment Management Services; and
- Monitoring Services: Device.

LAN Services and WAN Services – General

For all Customer-provided hardware receiving Managed Network Equipment Services, Customer will:

- Provide verification of licenses and necessary license keys applicable to Customer-provided software;

- Provide Sungard AS administrative and root level access;
- Obtain and maintain 24x7 maintenance agreements with the equipment vendor with 4 hour response time and notify the vendor of Sungard AS' authorization to act as Customer's agent under the maintenance agreements; and
- For equipment located at a Customer premises, Customer will provide physical and logical access as reasonably required by Sungard AS to perform the Services.

Sungard AS is not responsible for resolution of failures associated with i) hardware or software that is end of life or not otherwise supported by the vendor; or ii) Customer written or other software not supported by Sungard AS.

B. VAULTING SERVICES

Vaulting Services – Features

Sungard AS will perform the following, in accordance with the Customer completed design requirements form, for the data storage amount on the vaulted centralized off-site automated disk-to-disk back-up data protection ("Vault") at the Designated Sungard AS Facility, each as identified in the Order:

- Remote assistance with the initial installation and configuration of the third party software ("Vaulting Software") on each of Customer's source server(s) identified in the Order;
- Seeding of the Customer's data to the Vault ;
- Training Customer on the use of the Vaulting Software;
- Purging Customer-requested data sets from the Vault; and
- Access to Service generated backup reports.

Vaulting Services – General

Storage in excess of the data storage amount identified in the Order will result in the additional usage fee stated in the Order.

Seed and Restore Services – Features

Sungard AS will ship a removable disk-based storage device (based on the Customer identified storage size and interface type) to the Customer specified address to facilitate the transfer or restoration of large amounts of Customer's data.

Express Recovery Appliance Services – Features

Sungard AS will perform the following, in accordance with the Customer completed design requirements form, for the number of Express Recovery Appliances and the amount of committed storage, each as identified in the Order:

- Installation of the preconfigured Express Recovery Appliance as a local Vault at the Customer premises;
- Backups on the Express Recovery Appliance for a maximum of seven (7) days based on Customer configured backup schedule and retention policy;
- Replication of backups from the Express Recovery Appliance backups to the Vault at the Designated Sungard AS Facility; and
- Maintenance of the Express Recovery Appliance.

Plug-n-Protect Appliance Services – Features

Sungard AS will perform the following, in accordance with the Customer completed design requirements form, for the number of Plug-n-Protect Appliances and the amount of committed storage, each as identified in this Order:

- Installation of the preconfigured Plug-n-Protect Appliance as a local Vault at the Customer premises;
- Backups on the Plug-n-Protect Appliance based on Customer configured backup schedule and retention policy;
- Replication of backups from the Plug-n-Protect Appliance backups to the Vault at the Designated Sungard AS Facility; and
- Maintenance of the Plug-n-Protect Appliance.

Recover2Cloud™ for Vaulting – Features

Sungard AS will provide the following, in accordance with the Customer completed design requirements form, for the number of servers ("Protected Servers") identified in the Order:

- Remote access to Customer applications and data recovered from the Customer-contracted Vaulting Services to the virtual resource pool identified in the Order during a Vaulting Test or Disaster. A "Disaster" is defined as any unplanned event or condition that renders Customer unable to use the Protected Servers for their intended computer processing and related purposes;
- The number and duration of tests of the recovery of Customer applications and data identified in this Order that allow Customer to validate use of its data and applications following such recovery (each a "Vaulting Test"); and
- Deletion of Customer data and applications from the virtual resource pool following the conclusion of a Disaster or Vaulting Test.

Recover2Cloud for Vaulting – General

Customer will provide its Disaster Declaration notice to Sungard AS in the manner described in the Users' Guide and will specify the Services identified on this Order required by Customer. A "Disaster Declaration" is the notification provided by one of Customer's designated representatives to Sungard AS indicating that a Disaster has occurred. Sungard AS will provide access to the Users' Guide via the Customer Portal <http://www.mysungardas.com>.

Customer will:

- Provide Sungard AS with encryption keys necessary for Sungard AS to restore Customer data and applications from the Vault during a Vaulting Test or Disaster;
- Duplicate any changes performed in Customer's production configuration to the recovery configurations;
- Manage failback of Customer data and applications from the virtual resource pool following a Vaulting Test or Disaster;
- With respect to IBMi Protected Servers, provide Save System ("SAVSYS") files necessary for data and application restoration prior to implementation of the Services and each time the Protected Servers' operating systems are upgraded; and
- Comply with Sungard AS' Change Management and Notification Policy, located in the Customer Portal, and related to changes to Protected Server configurations (such as patches applied, upgrade of software, changes in IP address, etc.).

One or more other customers ("other affected customers") may declare a disaster and require use of the same Recover2Cloud Vaulting Resources at the same time as Customer ("Multiple Disaster"). The following provisions are intended to avoid or minimize contention for Recover2Cloud Vaulting Resources during a Multiple Disaster. "R2C Vaulting Resources" are the facilities, equipment, network and other resources used to provide the Recover2Cloud for Vaulting Services identified on this Order.

- All R2C Vaulting Resources are designated by Sungard AS as "Priority Resources" or "Shared Resources" and are subject to change without notice, provided that Sungard AS shall not change the designation of an R2C Vaulting Resource at any time that a customer is using such resource during a disaster;
- Customer will have priority rights of access to and use of R2C Vaulting Resources designated by Sungard AS as Priority Resources that are not then being used by other affected customers who previously declared disasters;
- Customer and all other customers experiencing a disaster will have equal rights of access to and use of Shared Resources, irrespective of the order in which disasters occur or are declared and, in such cases, Customer will reasonably cooperate with Sungard AS and the other affected customers in the use of the Shared Resources; and
- Sungard AS will maintain records of its receipt of disaster declarations, which will be the exclusive basis for determining the order in which disasters are declared

Customer may use the the R2C Vaulting Resources for 30 days following a Disaster Declaration. If a Disaster continues for longer than the 30 day period, Customer may continue to use the R2C Vaulting Resources; provided that this extended use is subject to immediate termination if and when any other customer declares a disaster and requires use of the same R2C Vaulting Resources that Customer is using.

Customer will comply with Sungard AS' Test Scheduling & Cancellation Policy set forth in the Customer Portal. All Vaulting Tests are subject to immediate cancellation by Sungard AS if and when any other customer declares a disaster and requests use of the Recover2Cloud Vaulting Resources being tested. Any such cancelled Vaulting Test will be rescheduled as soon as possible.

C. RECOVER2CLOUD SERVICES

Recover2Cloud for Server Replication – Features

Sungard AS will provide the following, in accordance with the Customer completed design requirements form, for the number of servers or LPARs ("Protected Assets") identified in the Order:

- Upon Customer request, analysis of the bandwidth between the Protected Assets and Sungard AS infrastructure required to support replication of Customer's applications and data;
- Assistance (if required) for installation and configuration of software agents on the Protected Assets;
- In addition to the site-to-site VPN connectivity identified in the Order, 2 site-to-site VPN connections between the Protected Assets and the Sungard AS storage system will be provided;
- Replication of Customer applications and data from the Protected Assets to Sungard AS' Recover2Cloud infrastructure and storage of such applications and data in the amount of storage identified in the Order;
- Monitoring and management of the replication process; Customer notification of replication and storage detected errors and threshold levels exceeded continuously for longer than 4 hours;
- Remote access to Customer applications and data recovered from the Sungard AS Recover2Cloud infrastructure to the virtual resource pool(s) identified in the Order during a Replication Test or Activation;
- Assistance in the failback of Customer applications and data from the virtual resource pool(s) to the Protected Assets following an Activation; and
- The quantity and duration of tests identified in the Order for Customer to validate recoverability of its data and applications (each a "Replication Test");

Recover2Cloud for Server Replication – General

Customer will provide its Activation notice to Sungard AS in the manner described in the Users' Guide. An "Activation" is the notification provided by one of Customer's designated representatives to Sungard AS indicating that an Event has occurred. An "Event" is any planned or unplanned event or condition that renders Customer unable to use the Protected Assets for their intended computer processing and related purposes. Sungard AS will provide access to the Users' Guide via the Customer Portal <http://www.mysungardas.com>.

Customer will:

- Configure the VPN connection where the Protected Assets are located;
- Provide Sungard AS with access necessary to conduct bandwidth analysis, install patches, and monitor the software agents installed by Sungard AS;
- For Windows-based Protected Assets, provide a non-OEM version of Windows;
- Comply with Sungard AS' Recover2Cloud Change Management Policy, located in the Customer Portal, and related to changes to Protected Asset configurations (such as patches applied, upgrade of software, changes in IP address, etc.);
- Obtain Internet or other IP bandwidth from Sungard AS or a third party, adequate to support a daily average replication recovery point objective (RPO) as desired by the Customer;
- If necessary for Sungard AS to provide the services described in the Order, provide an adequate number of process server devices, machines or virtual machines for the purpose of replication adequate to support a daily average replication recovery point objective (RPO) as desired by the Customer; Maintain VMware versions, if applicable, operating systems supported by Sungard AS, and the underlying replication software (Customer will upgrade software if notified by Sungard AS of changes in version support); and
- Install and configure software agents on the Protected Assets (Sungard AS will provide assistance upon Customer request).

In the event that Sungard AS' bandwidth analysis indicates that the amount of bandwidth specified in the Order will not support Customer's stated replication point objective, Customer will have the option to contract for additional bandwidth or make adjustments to the stated recovery point objective.

One or more other customers ("other affected customers") may declare an event and require use of the same R2C SR Resources at the same time as Customer ("Multiple Activation"). "R2C SR Resources" are defined as the facilities, equipment, network and other resources used to provide the Recover2Cloud for Server Replication Services identified on this Order. The following provisions are intended to avoid or minimize contention for R2C SR Resources during a Multiple Activation:

- All R2C SR Resources are designated by Sungard AS as "Priority Resources". Customer will have priority rights of access to and use of R2C SR Resources that are not then being used by other affected customers who previously declared activations; and
- Sungard AS will maintain records of its receipt of activations, which will be the exclusive basis for determining the order in which activations are declared.

Customer may use the R2C SR Resources for 30 days following an Activation. If an Event continues for longer than the 30 day period, Customer may continue to use the R2C SR Resources; provided that this extended use is subject to immediate termination if and when any other customer declares an Event and requires use of the same R2C SR Resources that Customer is using.

Customer may use R2C SR Resources and non-R2C SR Resources for use in Customer Replication Tests. Customer will comply with Sungard AS' Test Scheduling & Cancellation Policy. All Customer Replication Tests are subject to immediate cancellation by Sungard AS if and when any other customer declares an activation and requests use of the R2C SR Resources being tested. Any such cancelled Customer Replication Test will be rescheduled as soon as possible.

Any resource use (CPU, Memory, Storage, or items contracted in the Order) in excess of the committed amount will result in the additional usage fee stated in the Order.

Recover2Cloud for SRM – Features

Sungard AS will provide the following recovery of applications and data from Customer's virtual machines, in accordance with the Customer completed design requirements documents, for the number of recovery virtual machines ("Recovery VMs") and the compute resource pools identified in the Order:

- Configuration of the initial recovery plan setup on Customer's protected storage environment, including fine tuning of the plan setup using a Sungard AS-performed recovery during the initial 60 days following the commencement date;
- Manage the replication and recovery of the Recovery VMs;
- Hosting and management of the Recovery VMs on either Sungard AS-provided servers dedicated to the Customer ("Always-On") Sungard AS-provided shared servers used by multiple customers ("On-Demand") each as identified on the Order;
- Customer notification of errors detected in the replicated storage environment;
- Perform testing of the recovery of Customer applications and data that allows Customer to validate use of its data and applications following such recovery (each a "Recovery Test"), in the case of Recover2Cloud for SRM provided using the On-Demand offering, the number and duration of such tests will be identified on the Order; and
- Deletion of any Customer data and applications from the Recovery VMs using the On-Demand offering following the conclusion of a Recovery Test or Disaster.

If indicated on the Order, Sungard AS will manage the replication of Customer's applications and data from Customer's physical machines.

Recover2Cloud for SRM – General

Within the 60-day period after the Order Commencement Date, Customer may terminate the Order, without penalty, by providing Sungard AS with written notice. Such termination must be effective no later than 60 days from the Order

Commencement Date ("Termination Date"). Customer shall be liable for payment of all One Time Fees and Monthly Fees for the period from the Service Commencement Date until the Termination Date.

Definitions:

"Disaster" is defined as any unplanned event or condition that renders Customer unable to use Customer infrastructure that accesses the storage devices located at the Customer premises for their intended computer processing and related purposes.

"R2C SRM Resources" are defined as the facilities, equipment, network and other resources (but excluding Customer dedicated servers provided as part of the Always-On offering) used to provide the Recover2Cloud for SRM.

"Disaster Declaration" is defined as the notification provided by one of Customer's designated representatives to Sungard AS indicating that a Disaster has occurred.

Customer will provide its Disaster Declaration notice to Sungard AS in the manner described in the Users' Guide and will specify the Services identified on the Order required by Customer. Sungard AS will provide access to the Users' Guide via the Customer Portal <http://www.mysungardas.com>.

Customer will:

- Unless separately contracted with Sungard AS, provide Sungard AS the target storage environment and the design requirement documents to maintain and monitor storage replication between the source storage devices and the target storage environment;
- Provide Sungard AS with snapped/de-crypted access to data stored in the target storage environment;
- Install the Sungard AS-specified software on the target storage environment by following the instructions provided during the initial recovery plan setup;
- Comply with Sungard AS' Change Management and Notification Policy, located in the Customer Portal, and related configuration changes to Customer's environment (such as patches applied, upgrade of software, changes in IP address, etc.).

One or more other customers ("other affected customers") may declare a disaster and require use of the same R2C SRM Resources at the same time as Customer ("Multiple Disaster"). The following provisions are intended to avoid or minimize contention for R2C SRM Resources during a Multiple Disaster:

- All R2C SRM Resources are designated by Sungard AS as "Priority Resources" or "Shared Resources" and are subject to change without notice, provided that Sungard AS shall not change the designation of a R2C SRM Resource at any time that a customer is using such resource during a disaster;
- Customer will have priority rights of access to and use of R2C SRM Resources designated by Sungard AS as Priority Resources that are not then being used by other affected customers who previously declared disasters;
- Customer and all other customers experiencing a disaster will have equal rights of access to and use of Shared Resources, irrespective of the order in which disasters occur or are declared and, in such cases, Customer will reasonably cooperate with Sungard AS and the other affected customers in the use of the Shared Resources; and
- Sungard AS will maintain records of its receipt of disaster declarations, which will be the exclusive basis for determining the order in which disasters are declared.

Customer may use the R2C SRM -Resources for 30 days following a Disaster Declaration. If a Disaster continues for longer than the 30-day period, Customer may continue to use the R2C SRM Resources; provided that this extended use is subject to immediate termination if and when any other customer declares a disaster and requires use of the same R2C SRM Resources that Customer is using.

Customer will comply with Sungard AS' Test Scheduling & Cancellation Policy set forth in the Customer Portal. All Storage Replication Tests are subject to immediate cancellation by Sungard AS if and when any other customer declares a disaster and requests use of the R2C SRM Resources being tested. Any such cancelled Recovery Test will be rescheduled as soon as possible.

Sungard AS may use onshore or offshore subcontractors to perform aspects of the Service delivery; however data will never leave the continental us and any offshore resources, should they be used, will never have access to customers'

data. For the R2C suite of product, Sungard only recovers up to the Server login prompt. All data on those servers will be protected by the customer using standard server log on id and password at a minimum and on-shore or off-shore resources will have no access to the customer data unless login id and password are provided by the customer.

All data will reside within the continental US.

D. STORAGE SERVICES

Managed Vaulting for NetApp Services– Features

Sungard AS will provide the following, in accordance with the Customer completed design requirements form, for the data storage amount identified in the Order:

- Online access to centralized off-site automated disk-to-disk backup (“Vault”) and restoration of Customer’s protected data based on Customer defined backup schedules and retention periods;
- Seeding of the Customer’s data to the Vault;
- Monitoring of Customer NetApp environment that is backed up to the Sungard AS Vault and monitoring of the replication processes;
- Creation of a writable copy of customer’s backed up data (Flexclone);
- The management and monitoring the backup of data to Customer’s NetApp environment using Sungard AS supported software agents;
- Assist Customer in Customer disaster recovery activities; and
- Completion of Customer changes requiring Sungard AS implementation to the customer design requirements form 2 days following the Customer request of the requested effective date for such change.

If requested by Customer, Sungard AS will copy data from the Vault to a disk shelf and ship the disk shelf to the Customer-specified address. Subject to availability, Sungard AS may provide the disk shelf or will advise Customer on the necessary specifications for the disk shelf and related hardware based on Customer identified configurations.

Managed Vaulting for NetApp Services– General

Customer will:

- Provide a Sungard AS-approved firewall;
- Execute successful regular local backups using NetApp SnapShots;
- Report to Sungard AS any errors during the execution of regular local backups;
- Maintain LUN and/or database consistency with NetApp-supported tools or scripts products producing a valid recovery SnapShot;
- Provide Sungard AS reasonable advance notice of anticipated non-typical large data change rates; and
- Procure and install necessary software and hardware needed to perform the Services;
- Allow Sungard AS connectivity and administrative level user access to the Customer NetApp environment as necessary for Sungard AS to perform the Service;
- Provide necessary space, power, network, environmental controls, and related infrastructure to support and maintain all hardware and software installed in the Customer location required to provide the Services
- Provide adequately sized network connectivity to Sungard AS facilities to perform the offsite data backup;
- Remove Customer data from, de-rack, pack and return to Sungard AS, at Customer expense, the Sungard AS-provided hardware and software (if any) according to Sungard AS’ reasonable instructions and within 30 days of the termination of the Service;
- Notwithstanding the General Conditions set forth below, Customer will complete and return the data deletion form provided by Sungard AS within 15 days of termination of the Service; if Sungard AS does not receive Customer’s completed form within that period of time, Sungard AS will permanently delete all Customer data residing on Sungard AS infrastructure.

Data restoration requests for reasons other than data loss or corruption are limited to 2 per month; additional requests may incur additional time and material based fees.

Sungard AS does not guarantee that replication will be completed within scheduled backup window(s) nor that data restoration will occur within a defined period of time. Sungard AS will notify customer if replication will not complete in requested window and assist in suggesting changes to Customer environment. Sungard AS is not responsible for backup or recovery failures caused by: customer maintenance; Customer use of or changes to Sungard AS replication procedures, or Customer infrastructure or Customer application failure.

Additional fees will be assessed for storage used by Customer in excess of the committed capacity identified in the Order.

Managed Vaulting for Avamar® Services – Features

Sungard AS will provide the following, in accordance with the Customer completed design requirements form, for the data storage amount identified in the Order:

- Online access to a centralized firewall protected off-site automated disk-to-disk backup (“Vault”) via a VPN tunnel and restoration from the Vault of Customer’s protected Avamar data based on Customer defined backup schedules and retention periods;
- Seeding of the Customer’s data to the Vault;
- Creation of a recoverable copy of Customer’s Avamar backup for disaster recovery purposes;
- Initiation of Customer changes requiring Sungard AS implementation to the Customer design requirements form 2 days following the Customer request of the requested effective date for such change;
- Maintenance of all necessary software patch upgrades to the Vault;
- Notification in the event of a failure to replicate to the Vault;
- Daily backup reports provided to the Customer outlining which backup jobs completed or failed; and
- Capacity notification when Customer’s data usage reaches certain percentages of usage.

If requested by Customer, Sungard AS will copy of Customer’s backed up data from the Vault to via FTP or secure email or, if the quantity of data makes such delivery impractical, data will be copied to an appliance to be shipped to the Customer-specified address subject to an appliance rental fee.

Managed Vaulting for Avamar Services – General

Customer will:

- Maintain the Avamar software to the Sungard AS specified version;
- Provide a Sungard AS-approved firewall at the Customer location;
- Execute successful regular local backups using Avamar agents on protected servers;
- Report to Sungard AS any errors during the execution of regular local backups;
- Provide Sungard AS reasonable advance notice of anticipated non-typical large data change rates;
- Procure and install any necessary software and hardware needed at the Customer location to perform the Services;
- Allow Sungard AS connectivity and administrative level user access to the Customer Avamar environment as necessary for Sungard AS to perform the Service;
- Provide necessary space, power, network, environmental controls, and related infrastructure to support and maintain all hardware and software installed in the Customer location required to provide the Services;
- Provide adequately sized network connectivity from the Avamar environment in the Customer location to the Internet;
- Remove Customer data from, de-rack, pack and return to Sungard AS, at Customer expense, any Sungard AS-provided hardware and software according to Sungard AS’ reasonable instructions and within 30 days of the termination of the Service; and
- Notwithstanding the General Conditions set forth below, Customer will complete and return the data deletion form provided by Sungard AS within 15 days of termination of the Service; if Sungard AS does not receive Customer’s completed form within that period of time, Sungard AS will permanently delete all Customer data residing on Sungard AS infrastructure.

Sungard AS does not guarantee that replication will be completed within scheduled backup window(s) nor that data restoration will occur within a defined period of time. Sungard AS will notify Customer if replication will not complete in

requested window and assist in suggesting changes to Customer environment. Sungard AS is not responsible for backup or recovery failures caused by: Customer maintenance; Customer use of or changes to Sungard AS replication procedures, or Customer infrastructure or Customer application failure.

Additional fees will be assessed for storage used by Customer in excess of the committed capacity identified in the Order.

E. SERVICE CONDITIONS

| |
|--|
| Network Services |
| All hardware and software will be provided by Customer unless otherwise identified in the Order. Sungard AS does not guarantee a time to fix hardware or software. Sungard AS will engage and manage vendors in accordance with the terms of the underlying maintenance agreement and is not responsible for vendor failure to deliver parts or repairs within maintenance agreement timelines. |
| Vaulting Services |
| Sungard AS' delivery of the Vaulting Services involves a third party vendor, and with respect to the limitation of liability and Customer indemnification obligations contained in the Agreement, the third party vendor shall be deemed "Sungard AS". |
| <p>Customer will:</p> <ul style="list-style-type: none"> • Secure and maintain telecommunication connectivity between the Customer premises where the source servers are located and the Designated Sungard AS Facility; • Encrypt all Customer data transmitted and stored using the Services; and • Execute regular back-ups using the Vaulting Software and to report any errors in executing such back-ups; and • Configure and implement Customer desired changes to the data sets backed up to the Vault, the frequency of backups to the Vault, and data retention periods within the Vault. |
| <p>With respect to the third party software used to provide the Vaulting Services ("Vaulting Software"):</p> <ul style="list-style-type: none"> • The Vaulting Software is licensed directly by the third party provider to Customer and is subject to the third party provider's license agreement ("EULA"), a copy of which is available to Customer at the Customer Portal; • In the event that Sungard AS installs or configures the Vaulting Software on behalf of Customer, Customer is deemed to have taken such actions and to have accepted the EULA; • Vaulting Software upgrades, releases and/or patches are provided, to the extent available, directly by the Vaulting Software vendor Customer is responsible for implementing such changes to Customer servers on which the Vaulting Software is installed; • All rights not specifically granted to Customer herein are expressly reserved for the Vaulting Software vendor. The Vaulting Software and all intellectual property rights therein are the exclusive property of the Vaulting Software vendor; and • Upon termination or expiration of the Vaulting Services for any reason, all license rights in the Vaulting Software will immediately terminate and Customer will: (i) discontinue all use of the Vaulting Software; (ii) erase all copies of the Vaulting Software from Customer's equipment; and (iii) return all Vaulting Software media, manuals or access keys to Sungard AS within 30 days. |
| <p>For all appliances or devices shipped to Customer:</p> <ul style="list-style-type: none"> • Customer will pay all costs related to the shipping of the appliances or devices and risk of loss of the appliances or devices is Freight On Board from Sungard AS' or Sungard AS' third party provider premises; <ul style="list-style-type: none"> • Maintenance of the appliances or devices is provided by a third party vendor and Customer maintenance requests should be communicated directly to such third party; • Notwithstanding the included third party maintenance, the appliances and devices are provided to Customer "AS IS, WHERE IS" and Customer's only recourse for any warranty or indemnification related to the appliances lies with the third party maintenance vendor; • If Customer elects to purchase appliances or devices, Sungard AS retains a purchase money security interest therein until Sungard AS receives full payment for the items, and Customer shall promptly execute documents related thereto as requested by Sungard AS; and <ul style="list-style-type: none"> • If Customer does not pay the fees under this Order when due, then, in addition to its other remedies, Sungard AS shall be entitled to repossess the appliances or devices. |

| |
|-----------------------------------|
| General Service Conditions |
|-----------------------------------|

| |
|--|
| Sungard AS will provide technical support, problem resolution and change management in accordance its Support and Change Management Policy located in the Customer Portal. |
|--|

| |
|---|
| Sungard AS shall perform such janitorial services, environmental systems maintenance, power maintenance and other services as are reasonably required to maintain the Sungard AS facilities used to provide Services. |
|---|

| |
|--|
| Customer represents and warrants that it has the full legal right to utilize any Customer-provided software. |
|--|

F. SERVICE LEVEL AGREEMENT ("SLA")

| Services – Notification | | | | | | | | | | | |
|---|---|---|---|---------------------------------------|-------|--------------------|-----|--------------------|-----|---------|-----|
| <p><u>Agreement.</u> Sungard AS will notify Customer, in the manner requested by Customer in the Customer Portal, within 15 minutes after Sungard AS has conducted reasonable preliminary investigation verifying that the Services or Customer equipment monitored by the Services are unavailable.</p> | | | | | | | | | | | |
| <p><u>Remedy.</u> If Sungard AS fails to meet the Notification SLA, Customer is entitled to a credit equal to 3% of the Order's Monthly Fee for each failure in a that month. In the event that Customer notifies Sungard AS, within the 15 minute period, regarding unavailability of equipment or Services, this remedy is not operational.</p> | | | | | | | | | | | |
| Network Services – Managed Internet Access | | | | | | | | | | | |
| <p><u>Agreement.</u> The Sungard AS connection to the carrier network interface will be available 99.99% of the time measured on a monthly basis by computing the total number of successful attempted connections to the carrier as a percentage of the total number of attempted connections.</p> | | | | | | | | | | | |
| <p><u>Remedy.</u> If Sungard AS fails to meet the Internet Access SLA, Customer is entitled to a credit as set forth below for each month in which the failure occurred:</p> <table> <tr> <th><u>Internet Availability</u> <u>Percentage</u></th><th><u>Service Credit</u> <u>(% of the Order's Monthly Fee)</u></th></tr> <tr> <td>≥99.9% and <99.99%</td><td>10%</td></tr> <tr> <td>≥99.5% and <99.9%</td><td>15%</td></tr> <tr> <td>≥99.0% and < 99.5%</td><td>25%</td></tr> <tr> <td>< 99.0%</td><td>50%</td></tr> </table> | | <u>Internet Availability</u> <u>Percentage</u> | <u>Service Credit</u> <u>(% of the Order's Monthly Fee)</u> | ≥99.9% and <99.99% | 10% | ≥99.5% and <99.9% | 15% | ≥99.0% and < 99.5% | 25% | < 99.0% | 50% |
| <u>Internet Availability</u> <u>Percentage</u> | <u>Service Credit</u> <u>(% of the Order's Monthly Fee)</u> | | | | | | | | | | |
| ≥99.9% and <99.99% | 10% | | | | | | | | | | |
| ≥99.5% and <99.9% | 15% | | | | | | | | | | |
| ≥99.0% and < 99.5% | 25% | | | | | | | | | | |
| < 99.0% | 50% | | | | | | | | | | |
| Network Services – Basic Internet Access | | | | | | | | | | | |
| <p><u>Agreement.</u> The Sungard AS connection to the carrier network interface will be available 99.9% of the time measured on a monthly basis by computing the total number of successful attempted connections to the carrier as a percentage of the total number of attempted connections.</p> | | | | | | | | | | | |
| <p><u>Remedy.</u> If Sungard AS fails to meet the Internet Access SLA, Customer is entitled to a credit as set forth below:</p> <table> <tr> <th><u>Internet Availability</u> <u>Percentage</u></th><th><u>Service Credit</u> <u>(% of Basic Internet Service Monthly Fee)</u></th></tr> <tr> <td>≥99.5% and <99.9%</td><td>10%</td></tr> <tr> <td>≥99.0% and < 99.5%</td><td>15%</td></tr> <tr> <td>< 99.0%</td><td>25%</td></tr> </table> | | <u>Internet Availability</u> <u>Percentage</u> | <u>Service Credit</u> <u>(% of Basic Internet Service Monthly Fee)</u> | ≥99.5% and <99.9% | 10% | ≥99.0% and < 99.5% | 15% | < 99.0% | 25% | | |
| <u>Internet Availability</u> <u>Percentage</u> | <u>Service Credit</u> <u>(% of Basic Internet Service Monthly Fee)</u> | | | | | | | | | | |
| ≥99.5% and <99.9% | 10% | | | | | | | | | | |
| ≥99.0% and < 99.5% | 15% | | | | | | | | | | |
| < 99.0% | 25% | | | | | | | | | | |
| Network Services – Network Hardware Availability | | | | | | | | | | | |
| <p><u>Agreement.</u> Network hardware components provided by Sungard AS as part of Managed Firewall Services, Managed Intrusion Prevention (Network) Services, Managed Intrusion Detection (Network) Services, Unified Threat Management Standard and High Availability Services, LAN Equipment Services, WAN Equipment Services and Managed Load Balancing Services shall be operational and available to Customer on a monthly basis as set forth below:</p> <table> <tr> <td>Redundantly configured components</td><td>99.95%</td></tr> <tr> <td>Non-Redundantly configured components</td><td>99.5%</td></tr> </table> <p>Sungard AS shall measure the network at 5 minute intervals and, on a monthly basis, compute the number of failed measurement responses as a percentage of the total number of measurements.</p> | | Redundantly configured components | 99.95% | Non-Redundantly configured components | 99.5% | | | | | | |
| Redundantly configured components | 99.95% | | | | | | | | | | |
| Non-Redundantly configured components | 99.5% | | | | | | | | | | |
| <p><u>Remedy.</u> If Sungard AS fails to meet the Network Hardware SLA for 2 months in any 3 consecutive month period, Customer is entitled to a credit equal to 10% of the the Order's Monthly Fee for each month in which the failure occurred.</p> | | | | | | | | | | | |

| Vaulting Services – Vault Availability |
|--|
| <p>Agreement. The Vault shall be operational and available for Customer data transmission 99.99% of the time (“Vault Availability”). Vault Availability will be measured on a monthly basis utilizing internal monitoring software.</p> |
| <p>Remedy. If Sungard AS fails to meet the Vault Availability SLA, Customer is entitled to a credit equal to 10% of the Order's Monthly Fee for the month in which the failure occurs.</p> |
| Recover2Cloud for Vaulting Recovery Time Objective (RTO) |
| <p>Agreement. Sungard AS will recover and make available to Customer, Customer applications and data within 24 hours of commencement of a Disaster Declaration or Vaulting Test; provided that, this SLA does not amend, modify or otherwise alter the Multiple Disaster provisions concerning Recover2Cloud Vaulting Resource use and allocation. The SLA does not apply if Customer i) fails to correctly vault its data and applications; ii) uses non-current versions of the Vaulting Software or fails to apply Vaulting Software patches and updates; or iii) makes changes to Protected Server configurations not in compliance with Sungard AS' Change Management and Notification Policy.</p> |
| <p>Remedy. If Sungard AS fails to meet the Recover2Cloud for Vaulting RTO SLA, Customer is entitled to a credit equal to the Monthly Fee for the month in which the failure occurs. Notwithstanding the termination right described below in the “SLA Conditions”, Customer may terminate this Order if Sungard AS fails to meet the Recover2Cloud Vaulting RTO SLA 2 times within any 12 month period by providing Sungard AS advance written notice no later than 60 days following the second SLA failure.</p> |

Managed Vaulting for NetApp Services – Vault Availability

Agreement. The Vault shall be operational and available for Customer data transmission 99.5% of the time (“Vault Availability”). Vault Availability will be measured on a monthly basis utilizing internal monitoring software.

Remedy. If Sungard AS fails to meet the Vault Availability SLA, Customer is entitled to a credit equal to 10% of the Order’s Monthly Fee for the month in which the failure occurs.

Managed Vaulting for NetApp Services – Flexclone Creation SLA

Agreement. If Customer receives Recovery Services from Sungard AS, then Sungard AS will make Customer’s data vaulted using the Managed Vaulting for NetApp Services available for use with such Recovery Services within 2 hours of the commencement of a Test of or Disaster declaration requiring those Recovery Services.

Remedy. If Sungard AS fails to meet the Flexclone Creation SLA, Customer is entitled to a credit equal to the Order’s Monthly Fee for the month in which the failure occurs.

Managed Vaulting for Avamar Services – Vault Availability

Agreement. The Vault shall be operational and available for Customer data transmission 99.5% of the time (“Vault Availability”). Vault Availability will be measured on a monthly basis utilizing internal monitoring software.

Remedy. If Sungard AS fails to meet the Vault Availability SLA, Customer is entitled to a credit equal to 10% of the Order’s Monthly Fee for the month in which the failure occurs.

Managed Vaulting for Avamar Services – Backup Data Availability

Agreement. If Customer receives Recovery Services from Sungard AS, then Sungard AS will make Customer’s data vaulted using the Managed Vaulting for Avamar Services available for restoration with such Recovery Services within 2 hours of the commencement of a Test of or Disaster declaration requiring those Recovery Services.

Remedy. If Sungard AS fails to meet the Data Availability SLA, Customer is entitled to a credit equal to the Order’s Monthly Fee for the month in which the failure occurs.

Recover2Cloud for Server Replication Recovery Time Objective (RTO)

Agreement. Sungard AS will recover and make available to Customer Protected Assets upon commencement of Activation; provided that this SLA does not amend, modify or otherwise alter the Multiple Activation provisions concerning R2C SR Resource use and allocation. The SLA does not apply if Customer makes changes to Protected Assets configurations not in compliance with Sungard AS’ Recover2Cloud Change Management Policy.

| Quantity of | | |
|------------------|----------|----------------|
| Protected Assets | Platform | RTO (in-hours) |
| <=50 | x86 | 4 * |
| <= 5 | iSeries | 4 ** |
| <= 5 | AIX | 12 ** |
| <= 5 | Solaris | 12 ** |

* 1 additional hour for each additional 25 Protected Assets

** 1 additional hour for each additional 2 Protected Assets

Remedy. If Sungard AS fails to meet the Recover2Cloud for Server Replication RTO SLA, Customer is entitled to a credit equal to the Monthly Fee for the month in which the failure occurs. Notwithstanding the termination right described below

in the "SLAs General", Customer may terminate the Order if Sungard AS fails to meet the Server Replication RTO SLA 2 times within any 12 month period by providing Sungard AS advance written notice no later than 60 days following the second SLA failure.

Recover2Cloud for SRM RTO

Agreement. Sungard AS will recover the most recent copy of Customer's applications and data within the time frames set forth below of commencement of a Disaster Declaration or Recovery Test; provided that, this SLA does not amend, modify or otherwise alter the Multiple Disaster provisions concerning R2C SRM Resource use and allocation. The SLA does not apply if Customer i) fails to correctly replicate its data and applications; ii) uses software and hardware not supported by Sungard AS; iii) uses any backup or de-duplication technology that requires restoration in conjunction with storage replication; and iv) makes configuration changes to Customer's environment not in compliance with Sungard AS' Change Management and Notification Policy.

| <u>Quantity of Recovery VMs</u> | <u>Always-On RTO</u> <u>(in hours)</u> | <u>On-Demand RTO</u> <u>(in hours)</u> |
|---------------------------------|---|---|
| ≤ 250 | 4 | 8 |
| ≤ 500 | 6 | 10 |
| ≤ 750 | 8 | 12 |
| ≤ 1,000 | 10 | 16 |

Remedy. If Sungard AS fails to meet the Recovery as a Service RTO SLA, Customer is entitled to a credit equal to the Monthly Fee for the month in which the failure occurs. Notwithstanding the termination right described below in the "SLAs General", Customer may terminate the Order if Sungard AS fails to meet the Storage Replication RTO SLA 2 times within any 12 month period by providing Sungard AS advance written notice no later than 60 days following the second SLA failure.

SLAs General

If Sungard AS fails to meet an SLA, Customer is entitled to receive the applicable credit as Customer's sole monetary remedy (provided that the foregoing does not prohibit or limit Customer from seeking remedies for any breaches of other terms of the Contract related to such failure).

In no event will the total credits for all occurrences during a month exceed the Order's then current Monthly Fee.

Sungard AS will not be responsible for the failure to meet an SLA if the failure is caused by:

- A breach of the Contract by Customer, its employees, subcontractors or agents ("Customer Representatives");
- The negligence or intentional acts or omissions of Customer or Customer Representatives (including Customer retention of root or admin access and changes to data or configurations);
- Scheduled maintenance (including upgrades, repair or component replacement or scheduled backups) or other mutually agreed-to downtime;
- In the case of Enterprise Cloud Services, the absence of a patch, repair, policy, configuration or maintenance change recommended by Sungard AS but not approved by Customer, or configurations or architectures that are not supported or recommended by the applicable vendor; or
- Except in the case of Enterprise Cloud Services, equipment malfunction (provided said equipment has been maintained by Sungard AS in accordance with the terms of the Agreement), scheduled maintenance (including upgrades, repair or component replacement or scheduled backups) or other mutually agreed-to downtime, or the failure of any software to perform in accordance with its specifications ("Software Failure") and such Software Failure is not caused by Sungard AS' negligence, willful misconduct or failure to maintain a maintenance contract on such software. In the event of a Software Failure, if in the reasonable discretion of Sungard AS and Customer, such Software Failure cannot be corrected, Customer may, terminate the Order without penalty, upon written notice to Sungard AS